## REMARKS

In the Office Action dated January 3, 2005, claims 13-23 were rejected. Claims 13-23 are now pending in the application. In view of the remarks and amendments, Applicants respectfully request reconsideration of the application.

The Specification was objected to for informalities on pages 14 and 17. Applicant has corrected these items.

Claims 16 and 21 are objected to for a typographical error. Applicant has corrected these typographical errors.

Applicant acknowledges the Examiner's objections to Claims 19-23 if Claims 13, 14, and 16-18 were found allowable.

Claims 13-23 are rejected under U.S.C. § 112 as being indefinite. Applicant has corrected Claims 13-23 to overcome this rejection.

Claims 13, 16, 19 and 21 were rejected under U.S.C. § 103(a) as being unpatentable over the Koopman reference (US Patent 5,696,828) in view of the Wilson reference (US Patent 5,295,188).

However, in marked contrast to the Koopman reference and the Wilson reference both singly and in combination, amended Claims 13 and 19 include the limitation, in part, of:

> wherein each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value

The Examiner recites sections column 5, line 60-column 6, line 22 and column 7, lines 22-33 from the Koopman reference for the portions of Claims 13

and 19: shuffling a plurality of large random secrets and forming a plurality of shuffled large random secrets.

For example, the Koopman reference recites that the first function performed by the microprocessor is the algorithmic step of shuffling each data set. Further, upon receiving a digital data set of each converted sample, the microprocessor positions the digital data set into an array. (Koopman, column 5, line 60-column 6, line 22)

The Koopman reference further states that to insure randomness of the numbers generated by the system, an additional algorithmic step is performed. A portion of each compressed sample are input into an exclusive OR simultaneously with an independently varying, guaranteed non-repeating value such as the date and time of day. (Koopman, column 7, lines 22-33)

In marked contrast to the Koopman reference, the invention as described in Claims 13 and 19 perform nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets. Further, each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value.

Although the Koopman reference teaches shuffling a data set, the Koopman reference fails to teach nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets wherein each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value, as recited in Claims 13 and 19.

In fact, the Koopman reference teaches away from the invention as recited in Claims 13 and 19 by teaching that the use of "an independently varying, guaranteed non-repeating value such as the date and time of day" as an input to

the exclusive OR function. (Koopman, column 7, lines 22-33) Although unique, this "non-repeating value, such as the date and time of day" that is utilized as an input to the exclusive OR function is not random according to the Koopman reference. In marked contrast to the invention as recited in Claims 13 and 19, "each of the plurality of large random secrets is a random value and further the plurality of shuffled large random secrets are each a random value" are limited to random values and differ from the Koopman reference.

Further, the Wilson reference fails to teach nested shuffling each of a plurality of large random secrets, using a plurality of mixing keys thus forming a plurality of shuffled large random secrets wherein each of the plurality of large random secrets is a random value and further wherein the plurality of shuffled large random secrets are each a random value, as recited in Claims 13 and 19.

Accordingly, Applicants respectfully submit that the Koopman reference and the Wilson reference either singly or in combination fail to hint, teach, or suggest the elements within independent Claims 13 and 19. Thus, independent Claims 13 and 19 are patentable over the Koopman reference in view of the Wilson reference and are now in condition for allowance. In addition, Claims 16 and 21 depend directly or indirectly on Claims 13 and 19, respectively and, therefore, are patentable for at least the same reasons discussed above.

Claims 14, 15, and 20 were rejected under U.S.C. § 103(a) as being unpatentable over the Koopman reference (US Patent 5,696,828) and the Wilson reference (US Patent 5,295,188) in view of the Ritter reference (US Patent 5,623,549).

Independent Claims 13 and 19 are patentable for the same reasons as discussed above. Claims 14 and 15 depend directly or indirectly on allowable independent Claim 13 and, therefore, are patentable for at least the same reasons discussed above. Claim 20 depends directly or indirectly on allowable

independent Claim 19 and, therefore, is patentable for at least the same reasons discussed above.

Claims 17, 18, 22, and 23 were rejected under U.S.C. § 103(a) as being unpatentable over the Koopman reference (US Patent 5,696,828) and the Wilson reference (US Patent 5,295,188) in view of the Schneier reference (Applied Cryptography).

Independent Claims 13 and 19 are patentable for the same reasons as discussed above. Claims 17 and 18 depend directly or indirectly on allowable independent Claim 13 and, therefore, are patentable for at least the same reasons discussed above. Claims 22 and 23 depend directly or indirectly on allowable independent Claim 19 and, therefore, are patentable for at least the same reasons discussed above.

In view of the foregoing remarks and amendments, Applicants respectfully submit that all pending claims are in condition for allowance. Such allowance is respectfully requested.

If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully requested to contact Richard H. Butler at (408) 425-3376.

Respectfully submitted,

Dated: 1/9/06

Richard H. Butler
Registration No. 40,932

Please Send Correspondence to:
Valley Oak Law
5655 Silver Creek Valley Road
#106
San Jose, CA 95138
(408)425-3376